

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Missouri

FILED

JUL 30 2018

U.S. DISTRICT COURT  
EASTERN DISTRICT OF MO  
ST. LOUISIn the Matter of the Search of  
Information associated with cellular telephone  
account 314-882-6170 that is stored at premises  
controlled by Verizon Wireless

Case No. 4:18 MJ 6236 PLC

## APPLICATION FOR A SEARCH WARRANT

I, Vincent Liberto, a federal law enforcement officer or an attorney for the government  
request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:  
Information associated with cellular telephone account 314-882-6170 that is stored at premises controlled by  
Verizon Wireless

located in the \_\_\_\_\_ District of NEW JERSEY, there is now concealed

## SEE ATTACHMENT A

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

## Code Section

## Offense Description

18 U.S.C. Section 922(u)

theft of a firearm from a licensed dealer

26 U.S.C. Section 5861(d)

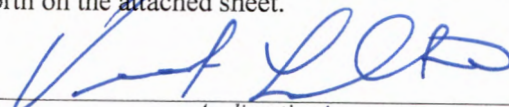
possession of a unregistered NFR firearm

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested  
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Vincent Liberto  
Special Agent, ATF

Printed name and title

Sworn to before me and signed in my presence.

Date: Julv 30. 2018

Judge's signature

City and state: St. Louis, MO

Honorable Patricia L. Cohen, U.S. Magistrate Judge

Printed name and title

AUSA: Rodney H. Holmes

FILED

JUL 30 2018

U.S. DISTRICT COURT  
EASTERN DISTRICT OF MO  
ST LOUIS

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Vincent N. Liberto, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Verizon Wireless, a wireless provider located at 180 Washington Valley Road, Bedminster, New Jersey 07921. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 2703(c)(1)(A) to require Verizon Wireless to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, not including the contents of communications, related to the account associated with cellular telephone number **314-882-6170** (hereinafter **subject cellular telephone**). The information to be seized is described in the following paragraphs and in Attachment A.

2. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court of the Eastern District of Missouri is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 922(u) and 26 U.S.C. § 5861(d) and “is in . . . a district in which the provider . . . is located or in which the wire or electronic communications, records, or other information are stored.” 18 U.S.C. § 2711(3)(A)(ii).

3. I am a Special Agent with the United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) since August 2016, currently assigned to the Kansas City Field Division, St. Louis Group I Field Office. Prior to my employment with ATF,

I was a Detective with Baton Rouge Police Department (BRPD) in Baton Rouge, Louisiana. I was employed with BRPD from 2008 to 2016. I currently conduct criminal investigations into cases of illegal possession / transfer of firearms, firearms trafficking, narcotics trafficking, and violent crimes. The facts alleged in this affidavit come from my own investigation, my training and experience, and information obtained from other investigators and witnesses. In my experience, I have been involved in criminal investigations wherein wireless communication and wireless communication data was used to successfully identify and locate suspects of investigations.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Further, by submitting this affidavit, your affiant is not conceding that a warrant issued upon a showing of probable cause is required to obtain the records requested herein. Rather, a warrant is being applied for in this case out of an abundance of caution due to potential future changes in the law of this Circuit.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 922(u) and 26 U.S.C. § 5861(d) have been committed by Gerimy PLUMMER and unknown associates. There is also probable cause to search the information for evidence of these crimes, as described in Attachment A.

#### **PROBABLE CAUSE**

6. ATF is currently involved in an investigation into the violation of a FFL burglary committed by Gerimy PLUMMER. Agents and officers are investigating a group of individuals in St. Louis who are engaged in firearms offenses and criminal activity. On June 6, 2018, at approximately 0230 hours, iTechshark, located at 14844 Manchester Road, Ballwin, Missouri

63011, was burglarized by two individuals wearing mask and hoods, long sleeves, and gloves. These two individuals arrived in a BMW four-door, dark colored, sedan, with dark rims. These individuals gained access to the interior of the store utilizing a landscaping brick to break the front glass door. Once inside, these two individuals stole several cellular telephones and computers/laptops.

7. Ballwin Police Department (BPD) was dispatched and responded to the burglar alarm at the iTechshark. When the first responding officer arrived on scene, this officer encountered the suspect vehicle fleeing the scene. The officer activated their emergency lights and sirens and attempted to stop the suspect vehicle. The suspect vehicle refused to stop and fled west bound on Manchester Boulevard. Due to the high speeds and reckless driving, BPD officer decided not to pursue the suspect vehicle. The BPD marked police unit was equipped with an in-car camera system. This in-car camera was able to capture distinctive characteristics of the suspect vehicle.

8. On June 6, 2018, at approximately 0315 hours, Adventure Shooting Sports (Federal Firearms Licensee # 636-539-6950), located at 17724 Chesterfield Airport Road, Chesterfield, Missouri 63055, was burglarized by two individuals wearing marks and hoods, long sleeves, and gloves. These individuals gained access to the interior of the store utilizing a large cast iron commercial pipefitting to break the front door glass. Once inside, these two individuals stole twenty-six firearms; to include the following NFA weapon: Daniel Defense, ISR, .300 caliber, suppressor, serial # ISR03024. These two individuals fled the scene prior to Chesterfield Police Department (CPD) arriving on scene.

9. ATF, BPD, and CPD began an investigation into these two burglaries. The following is what investigators learned up to the present date:

10. Investigators analyzed the interior surveillance footage from iTechshark and Adventure Shooting Sports. When comparing the two suspects in both burglaries there are several similarities in clothing type, clothing color, how the clothing is worn, height, and weight.

11. Surveillance video was obtained from a business nearby Adventure Shooting Sports; which captured the suspects and suspect vehicle. It shows the passenger of the suspect vehicle exiting the front passenger seat and attempting to pick up a landscaping brick. However, it appeared the landscaping brick was too heavy. The suspect continued to walk the parking lot. A short time later, the suspect returns to the suspect vehicle. The suspect vehicle is seen going behind another business. This is where the suspects located a crate filled with the same large cast iron commercial pipefitting used to break the front glass door at Adventure Shooting Sports.

12. The suspect vehicle in this surveillance video appeared to be the same suspect vehicle used in the iTechshark burglary and fled BPD officers.

13. Investigators consulted with a BMW dealership to determine a model and year for the BMW seen fleeing BPD. Investigators learned the BMW was a 2011-2012 i535 x-drive.

14. Investigators discovered a 2011 BMW i535 x-drive, Missouri license plate # YH3 N4M, VIN # WBAFU7C5XBC874092 was reported stolen in Saint Charles, Missouri on May 5, 2018. On June 6, 2018, at approximately 2030 hours, this same stolen vehicle was recovered at Mama Kaya apartment complex, located at 2800 Stoddard Street, Saint Louis, Missouri 63106.

15. Surveillance video at Mama Kaya apartments captured the stolen vehicle arriving in the parking lot at approximately 0515 hours on June 6, 2018. The following is the events the surveillance video captures:

16. The stolen BMW arrives with a front left flat tire. The stolen BMW is parked on the north side of the parking lot. The driver, suspect #1, exits the vehicle and walks towards the only entrance to the parking lot while on a cellular telephone. Suspect #1 is a black male, with



short hair, wearing a black short sleeve shirt with one sleeve white, black pants, white shoes, and a small bag with a single strap around his torso. It appears the driver is either looking for something/someone or waiting for someone. The driver then returns to the stolen BMW.

17. Approximately ten minutes later, a 2005 silver Pontiac Sunfire with a temporary Missouri license plate and distinctive damage on the exterior of this vehicle arrives at 2800 Stoddard Street. The front passenger, suspect #2, of the Pontiac exits the vehicle and walks towards the stolen BMW. Suspect #2 is a black male, wearing a blue Chicago Cubs shirt with the number "44" and what is believed to be the name "Rizzo" on the back. Suspect #2 appears to be smaller in stature than suspect #1. Suspect #1 exits the stolen BMW. It appears suspect #1 and suspect #2 begin to put objects in their pants. Suspect #1 is seen putting objects in the bag he is carrying. Both suspects walk back to the Pontiac. They both walk in an abnormal way, as if they are attempting to conceal objects in their pants. Both subjects enter the Pontiac and leave the parking lot.

18. Later the same day of June 6, 2018, a dark colored, newer model, Nissan four-door sedan arrives at 2800 Stoddard Street. The Nissan parks next to the stolen BMW. A black male subject, that reassembles suspect #1, exits the driver seat of the Nissan. This subject starts to wipe clean the exterior and interior of the BMW. He also removes a computer, a laptop, dark clothing, and other objects from the BMW and places these items into the Nissan. After this subject spends approximately fifteen minutes wiping clean the BMW, he returns to the Nissan and leaves the parking lot.

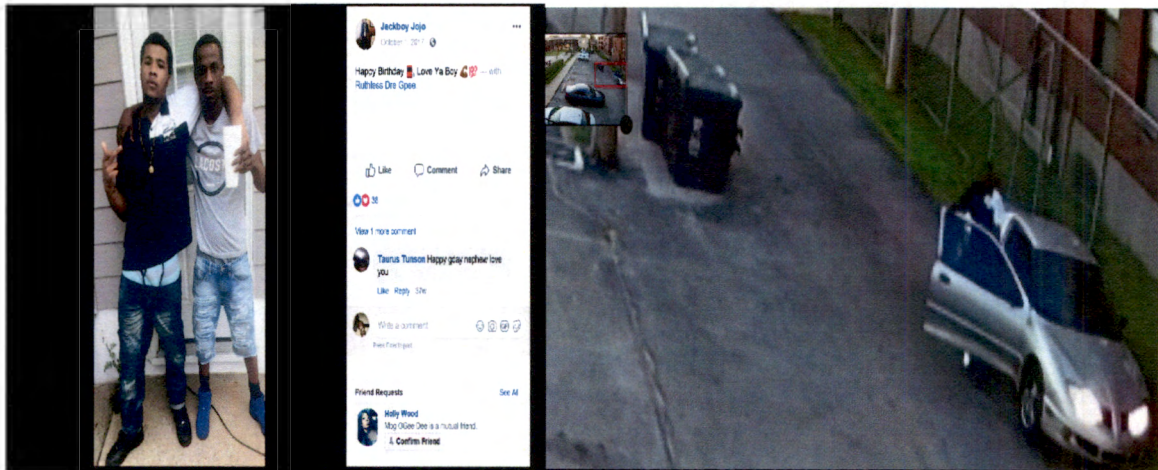
19. On June 19, 2018, ATF Saint Louis Group I and Saint Louis Metropolitan Police Department executed an unrelated state search warrant at a residence within the city limits of Saint Louis City. While at this search warrant, Investigators located the Pontiac, suspect #2, and the owner of the Pontiac. The owner of the Pontiac, identified as Maurice Davis, was shown a

photograph of suspect #1 taken from the surveillance video. Davis immediately, without hesitation, stated suspect #1 is "GP". Suspect #2, identified as Preston Bell, was shown a photograph of suspect #2 taken from the surveillance video. Bell admitted the suspect in the photograph wearing the Chicago Cubs shirt was him.

20. Investigators recognized from the surveillance video suspect #1 to be Gerimy PLUMMER, goes by the moniker "GP", DOB: 10-01-1998, FBI # C7TJTELNT. PLUMMER was utilizing a publicly available Facebook account, that being <https://www.facebook.com/ruthless.gpee>, Ruthless Dre Gpee, (ruthless.gpee) further described and identified as Facebook profile ID: 100013333727923.

21. This Facebook account was not private or restricted. It was readily viewed without being "friends" of the respective user. Investigators subsequently viewed portions of the respective account.

22. Investigators saw a photograph posted on this Facebook account with PLUMMER wearing the same shirt that suspect #1 was wearing at the time the stolen BMW was parked at 2800 Stoddard Street.



23. The day after Bell and Davis were interviewed, PLUMMER removed his Facebook account and is no longer available to be viewed or searched. On June 25, 2018, I applied for and obtained a federal search warrant for PLUMMER's Facebook account.

24. After reviewing PLUMMER's Facebook messages, I discovered PLUMMER was also utilizing the **subject cellular telephone** to communicate with others during the time period in question.

25. It is believed that PLUMMER utilized the **subject cellular telephone** in furtherance of criminal activity based upon the collective training and experience of the investigators. Investigators believe that PLUMMER would need to communicate with co-conspirators in making the plan for the burglary, planning the disposal of the stolen BMW, and storing or selling the stolen firearms. The information requested, will further the ongoing investigation.

26. In my training and experience, I have learned that Verizon Wireless is a company that provides cellular and data telephone access to the general public.

27. Wireless phone providers typically generate and retain certain transactional information about the use of each telephone, voicemail, data used, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

28. Many wireless phone providers generate and retain information about the location in which a particular communication was transmitted or received. Your affiant is aware, through



training and experience, and through consultation with agents with additional training or experience relating to wireless phone technology, that when a cellular device is used to make or receive a call, or text message, or other communication, the wireless phone provider will maintain a record of which cell tower was used to process that contact. In general, but not always, the cellular telephone at issue will use the closest unobstructed tower that generates the strongest signal. These wireless providers maintain this information, including the corresponding cell towers (i.e., antenna towers covering specific geographic areas), “sectors” (i.e., faces of the towers), and other signaling data, as part of their regularly conducted business activities. Typically, a wireless provider maintains a record of the cell tower information associated with calls. These cell tower records are sometimes referred to as “cell site” data.

29. Because the cellular device generally attempts to communicate with the closest unobstructed tower, by reviewing the above-described information, your affiant and other law enforcement officers can determine the approximate geographic area from which the communication originated or was received.

30. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), an International Mobile Subscriber Identifier (“IMSI”), or an International Mobile Station Equipment Identity (“IMEI”).

When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

31. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers' full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service used, the ESN or other unique identifier for the cellular device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates and times of payments and the means and source of payment (including any credit card or bank account number).

**INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

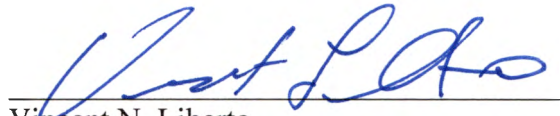
32. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. § 2703(c)(1)(A), by using the warrant to require Verizon Wireless to disclose to the government copies of the records and other information (excluding the content of communications) particularly described in Section I of Attachment A. Upon receipt of the information described in Section I of Attachment A, government-authorized persons will review that information to locate the items described in Section II of Attachment A.

33. Because the information is to be provided by Verizon Wireless and does not involve any physical intrusion by the government or any investigative agency, it is respectfully

suggested that the normal time constraints requiring that the warrant be executed only in the daytime are not applicable.

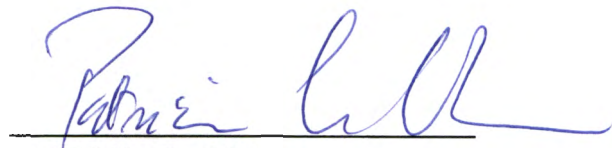
**CONCLUSION**

34. Based on the forgoing, I submit that there is probable cause to conclude that requested information associated with the cellular telephone having the number **314-882-6170**, as further described herein and in Attachment A, is available from Verizon Wireless and that information, including cell site information, constitutes evidence of violations of Sections 18 U.S.C. § 922(u) (FFL Burglary) and 26 U.S.C. 5861(d) (Possession of an unregistered NFA Weapon) by Gerimy PLUMMER and others known or unknown at this time. Accordingly, I respectfully request that the Court issue the proposed search warrant.



Vincent N. Liberto  
Special Agent  
Bureau of Alcohol, Tobacco, Firearms and Explosives

SUBSCRIBED and SWORN to before me this 30 day of July, 2018.



PATRICIA L. COHEN  
United States Magistrate Judge  
Eastern District of Missouri

## **ATTACHMENT A**

### **Particular Things to be Seized**

#### **I. Information to be disclosed by Verizon Wireless**

Verizon Wireless is required to disclose the following records and other information, if available, to the United States for (314) 882-6170 which are stored at premises owned, maintained, controlled, or operated by Verizon Wireless, a wireless provider located at 180 Washington Valley Road, Bedminster, New Jersey 07921 ("Account"), for the time period 06/05/2018 – 07/30/2018:

- A. The following information about the customers or subscribers of the Account:
  - 1. Names (including subscriber names, user names, and screen names);
  - 2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
  - 3. Local and long distance telephone connection records;
  - 4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
  - 5. Call Detail Records and Data Detail Records
  - 6. Length of service (including start date) and types of service utilized;
  - 7. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"));
  - 8. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
  - 9. Means and source of payment for such service (including any credit card or bank account number) and billing records.
- B. All records and other information (not including the contents of communications) relating to the Account, including:
  - 1. Information about each communication sent or received by the Account, including the date and time of the communication, the method of

- communication, and the source and destination of the communication (such as source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
2. All data about which “cell towers” (i.e., antenna towers covering specific geographic areas), “sectors” (i.e., faces of the towers), and (if available) “azimuth” received a radio signal from each cellular telephone or device assigned to the Account; and
  3. Records of user activity for each connection made to or from the Account, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 922(u) and 26 U.S.C. § 5861(d) involving Gerimy PLUMMER since June 5, 2018 to present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Burglary of Adventure Shooting Sports, located at 17724 Chesterfield Airport Road, Chesterfield, Missouri 63005,
- (b) Communications between Gerimy PLUMMER and unknown associates, and preparatory steps taken in furtherance of the scheme.
- (c) The identity of the person(s) who created or used the account or identifier, including records that help reveal the whereabouts of such person(s).
- (d) The identity of witnesses and/or co-conspirators with whom the account user communicated.



**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
BUSINESS RECORDS PURSUANT TO FEDERAL RULE  
OF EVIDENCE 902(11)**

I, \_\_\_\_\_, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Verizon Wireless, and my official title is \_\_\_\_\_. I am a custodian of records for Verizon Wireless. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Verizon Wireless, and that I am the custodian of the attached records consisting of \_\_\_\_\_ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Verizon Wireless; and
- c. such records were made by Verizon Wireless as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature